

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JC672 U.S. PTO
10/061174
02/04/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 3月 2日

出 願 番 号

Application Number:

特願2001-059042

[ST.10/C]:

[JP2001-059042]

出 願 人

Applicant(s):

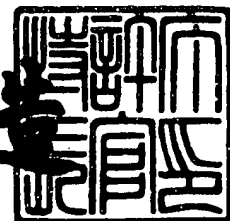
セイコーエプソン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 1月11日

特許庁長官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3114178

【書類名】 特許願

【整理番号】 J0083370

【提出日】 平成13年 3月 2日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明者】

 【住所又は居所】 長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

 【氏名】 山門 均

【特許出願人】

 【識別番号】 000002369

 【氏名又は名称】 セイコーエプソン株式会社

【代理人】

 【識別番号】 100093388

 【弁理士】

 【氏名又は名称】 鈴木 喜三郎

 【連絡先】 0266-52-3139

【選任した代理人】

 【識別番号】 100095728

 【弁理士】

 【氏名又は名称】 上柳 雅誉

【選任した代理人】

 【識別番号】 100107261

 【弁理士】

 【氏名又は名称】 須澤 修

【手数料の表示】

 【予納台帳番号】 013044

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9711684

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置及び当該情報処理装置の制御方法、並びに制御プログラム及び当該制御プログラムを記録したコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項 1】 固有の識別データを無線送信する可搬操作子と、

前記可搬操作子によって操作され、該操作を検出すると検出結果を出力する操作検出手段と、

識別データを記録する記録手段と、

前記可搬操作子から送信される識別データを受信する受信手段と、

前記受信手段により受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手段と、

前記判定手段により該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手段と、

前記認証手段により認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 固有の識別データを無線送信する可搬操作子と、

前記可搬操作子によって操作され、該操作を検出すると検出結果を出力する操作検出手段と、

ユーザデータと識別データを記録する記録手段と、

前記可搬操作子から送信される識別データを受信する受信手段と、

前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第 1 の判定手段と、

前記受信手段により受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第 2 の判定手段と、

前記第 1 の判定手段により該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第 2 の判定手段により該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られた

と判定する認証手段と、

前記認証手段により認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段と

を備えることを特徴とする情報処理装置。

【請求項 3】 可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有する情報処理装置の制御方法において、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、

前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段と

を有することを特徴とする情報処理装置の制御方法。

【請求項 4】 可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有する情報処理装置の制御方法において、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第 1 の判定手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第 2 の判定手順と、

前記第 1 の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第 2 の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段と

を有することを特徴とする情報処理装置の制御方法。

【請求項 5】 可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、
前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、
前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、
前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、
前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と
を実行させるための制御プログラム。

【請求項 6】 可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、
前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、
前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第 1 の判定手順と、
前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第 2 の判定手順と、
前記第 1 の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第 2 の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、
前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と
を実行させるための制御プログラム。

【請求項 7】 可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、

前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と

を実行させるための制御プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 8】 可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、

前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、

前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第 1 の判定手順と、

前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第 2 の判定手順と、

前記第 1 の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第 2 の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、

前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順と

を実行させるための制御プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置に関し、ユーザの認証を行う情報処理装置に関する。

【0002】

【従来の技術】

従来、パーソナルコンピュータやワークステーション等の情報処理装置においては、ログイン等の際にユーザ名とパスワードに基づいてユーザ認証を行っている。近年では、ユーザ名とパスワードに限らず、指紋などの生体情報を用いてユーザ認証を行う方法も提案されている。

【0003】

【発明が解決しようとする課題】

しかしながら、この種の情報処理装置においては、一端ユーザ認証が得られると、明示的にログアウトまたは電源がオフされるまでは誰でも使用できる状態になってしまう。このため、正規のユーザがログアウトせずに情報処理装置から離れた場合は、第三者に不正利用されるおそれがあった。

【0004】

また、ユーザ名とパスワードのみでユーザの認証を行う場合は、第三者にユーザ名とパスワードが知られてしまうと、正規のユーザに知られることなく第三者が正規のユーザになりすますことができる問題がある。

これらの場合にユーザの認証を繰り返し行う方法も考えられるが、パスワードなどの入力作業や指紋認証処理を何度も行う必要があり、使い勝手が悪くなってしまう問題が生じる。

【0005】

そこで本発明の目的は、簡易かつ確実に第三者の不正利用を防止することができる情報処理装置及び当該情報処理装置の制御方法、並びに制御プログラム及び該制御プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的としている。

【0006】

【課題を解決するための手段】

上記課題を解決するため、本発明は、固有の識別データを無線送信する可搬操作子と、前記可搬操作子によって操作され、該操作を検出すると検出結果を出力

する操作検出手段と、識別データを記録する記録手段と、前記可搬操作子から送信される識別データを受信する受信手段と、前記受信手段により受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手段と、前記判定手段により該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手段と、前記認証手段により認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段とを備えることを特徴としている。

【 0 0 0 7 】

この構成によれば、情報処理装置は、記録手段に記録された識別データと一致する識別データを送信する可搬操作子が近くに存在する間だけ各種操作に対応する処理を行うことにより、可搬操作子を所持する正規のユーザが近くに存在する間だけユーザの操作に対応する処理を行うことができる。

【 0 0 0 8 】

また、本発明は、固有の識別データを無線送信する可搬操作子と、前記可搬操作子によって操作され、該操作を検出すると検出結果を出力する操作検出手段と、ユーザデータと識別データを記録する記録手段と、前記可搬操作子から送信される識別データを受信する受信手段と、前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第1の判定手段と、前記受信手段により受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第2の判定手段と、前記第1の判定手段により該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第2の判定手段により該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手段と、前記認証手段により認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手段とを備えることを特徴としている。

【 0 0 0 9 】

この構成によれば、情報処理装置は、識別データの一致不一致の判定に加えて、入力されたユーザデータが記録手段に記録されたユーザデータと一致するか否

かを判定するので、さらに高い認証精度で正規のユーザが近くに存在する間のみユーザの操作に対応する処理を行うことができる。

【0010】

また、本発明は、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有する情報処理装置の制御方法において、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを有することを特徴としている。

【0011】

この構成によれば、情報処理装置は、記録手段に記録された識別データと一致する識別データを送信する可搬操作子が近くに存在する間だけ各種操作に対応する処理を行うことにより、可搬操作子を所持する正規のユーザが近くに存在する間だけユーザの操作に対応する処理を行うことができる。

【0012】

また、本発明は、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有する情報処理装置の制御方法において、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第1の判定手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第2の判定手順と、前記第1の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第2の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応

する処理を行う情報処理手順とを有することを特徴としている。

【0013】

この構成によれば、情報処理装置は、識別データの一致不一致の判定に加えて、入力されたユーザデータが記録手段に記録されたユーザデータと一致するか否かを判定するので、さらに高い認証精度で正規のユーザが近くに存在する間のみのユーザの操作に対応する処理を行うことができる。

【0014】

また、本発明は、制御プログラムにおいて、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを実行させることを特徴としている。

【0015】

このプログラムによれば、コンピュータは、記録手段に記録された識別データと一致する識別データを送信する可搬操作子が近くに存在する間だけ各種操作に対応する処理を行うことにより、可搬操作子を所持する正規のユーザが近くに存在する間だけユーザの操作に対応する処理を行うことができる。

【0016】

また、本発明は、制御プログラムにおいて、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第1の判定手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第2の判定手順と、前記第1の判定手順にお

いて該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第2の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを実行させることを特徴としている。

【0017】

このプログラムによれば、コンピュータは、識別データの一致不一致の判定に加えて、入力されたユーザデータが記録手段に記録されたユーザデータと一致するか否かを判定するので、さらに高い認証精度で正規のユーザが近くに存在する間のみユーザの操作に対応する処理を行うことができる。

【0018】

また、本発明は、コンピュータ読み取り可能な記録媒体において、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、前記受信手段が前記可搬操作子から送信される識別データを受信する受信手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する判定手順と、前記判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを実行させることを特徴としている。

【0019】

この記録媒体によれば、コンピュータは、記録手段に記録された識別データと一致する識別データを送信する可搬操作子が近くに存在する間だけ各種操作に対応する処理を行うことにより、可搬操作子を所持する正規のユーザが近くに存在する間だけユーザの操作に対応する処理を行うことができる。

【0020】

また、本発明は、コンピュータ読み取り可能な記録媒体において、可搬操作子と、可搬操作子の操作を検出する操作検出手段と、受信手段と、記録手段とを有するコンピュータに、前記受信手段が前記可搬操作子から送信される識別データ

を受信する受信手順と、前記操作手段の検出結果に基づいて入力されたユーザデータが前記記録手段に記録されたユーザデータと一致するか否かを判定する第1の判定手順と、前記受信手順において受信された識別データが前記記録手段に記録された識別データと一致するか否かを継続的に判定する第2の判定手順と、前記第1の判定手順において該入力されたユーザデータが該記録されたユーザデータと一致すると判定され、かつ、前記第2の判定手順において該受信された識別データが該記録された識別データと一致すると判定される間は、認証が得られたと判定する認証手順と、前記認証手順において認証が得られている間だけ、前記操作検出手段の検出結果に対応する処理を行う情報処理手順とを実行させることを特徴としている。

【 0 0 2 1 】

この記録媒体によれば、コンピュータは、識別データの一致不一致の判定に加えて、入力されたユーザデータが記録手段に記録されたユーザデータと一致するか否かを判定するので、さらに高い認証精度で正規のユーザが近くに存在する間のみユーザの操作に対応する処理を行うことができる。

【 0 0 2 2 】

【発明の実施の形態】

以下、適宜図面を参照しながら本発明の実施形態について説明する。

【 0 0 2 3 】

(1) 実施形態

(1. 1) 実施形態の構成

図1は、本発明の実施形態に係る情報処理装置1とこの情報処理装置1の操作を行うペン型操作子2の外観を示す図である。ペン型操作子2は、操作者がペンのように手に持って用いるポインティングデバイスである。情報処理装置1は、ペン型操作子2を持った操作者が机の上において操作したり、バックにいれて持ち運んで外出先で使用する装置である。

【 0 0 2 4 】

情報処理装置1は、略矩形形状の薄型のボディを持ち、その表面には略全面にわたって表示画面3が設けられている。表示画面3は、図2に示すように、液晶

表示パネル 3 a と、この液晶表示パネル 3 a の上面に設けられる透明のタッチパネル（操作検出手段） 3 b を有しており、ペン型操作子 2 によって表示画面 3 の表面が押圧されると、その位置がタッチパネル 3 b により検出されるようになっている。

【0025】

次に、図 3 を参照して、情報処理装置 1 とペン型操作子 2 の電氣的構成を説明する。

情報処理装置 1 において、CPU（判定手段、情報処理手段）10 は、ROM 12 に記録されたプログラムを読み出して実行することにより、この情報処理装置 1 全体の制御を行う。RAM 11 は、CPU 10 の制御の下に表示画面 3 に表示するイメージデータ等を一時的に格納するバッファメモリとして機能すると共に、各種データを一時記憶する。後述する処理に用いられる認証フラグ F もこの RAM 11 に設定される。ROM 12 は、CPU 10 が読み出して実行する各種プログラムやペン型操作子 2 の識別データ ID 等を記録するメモリである。フラッシュメモリ 13 は、CPU 10 の制御の下に各種データを不揮発状態で保持するメモリである。液晶駆動部 14 は、RAM 11 に記録されたイメージデータを読み出して対応する画像データを液晶表示パネル 3 a に表示させる。受信部 15 は、CPU 10 の制御の下にアンテナから入力したデータを受信し、受信データを CPU 10 に出力する。入出力部 16 は、CPU 10 の制御の下に入出力端子を介してインターネットに接続したり、パーソナルコンピュータ（PC）等と接続してデータ通信を行う。

【0026】

次に、ペン型操作子 2 の電氣的構成について説明する。ペン型操作子 2 において、メモリ 20 は、固有の識別データ ID を記録するメモリである。送信部 21 は、メモリ 20 に記録された識別データ ID をアンテナ 2 a（図 1 参照）から無線で送信させる。ここで、ペン型操作子 2 の送信部 21 と情報処理装置 1 の受信部 15 との間の通信方式には、短距離無線通信方式が適用され、ペン型操作子 2 が情報処理装置 1 の近傍（例えば数 m の範囲内）に存在する場合にのみ受信部 15 が識別データ ID を受信できるようになっている。この短距離無線通信方式に

は、例えば、マイクロ波方式、電磁誘導方式が適用され、変調方式には、スペクトラム拡散 (Spread Spectrum) 方式、周波数ホッピング (Frequency Hopping) 方式または直接拡散 (Direct Sequence) 方式等が適用される。

【 0 0 2 7 】

(1 . 2) 実施形態の動作

次に、この情報処理装置 1 の概略動作を説明する。

まず、この情報処理装置 1 の初期設定時の動作を説明について説明する。

電源ボタンが操作されて情報処理装置 1 の電源が初めて投入されると、CPU 10 は、初期設定処理を行う。この初期設定処理においては、CPU 10 は、液晶駆動部 14 により図 4 に示す登録画面 30 を表示画面 3 に表示させ、操作者によりペン型操作子 2 で表示画面 3 が押圧操作されると、表示画面 3 のタッチパネル 3 b から通知される押圧位置に基づいてユーザ名とパスワードの登録処理を行う。

【 0 0 2 8 】

具体的には、CPU 10 は、押圧位置がユーザ名の入力欄 30 a またはパスワードの入力欄 30 b 内であると判定した場合は、各入力欄 30 a または 30 b の対応する位置にカーソルを点滅させる。また、CPU 10 は、押圧位置が文字パレット 30 c 内の文字等であると判定した場合は、その文字等を入力欄 30 a または 30 b のカーソル点滅位置に表示させる一方、押圧位置が削除ボタン 30 d であると判定した場合は、入力欄 30 a または 30 b のカーソル点滅位置にある文字等を消去させる。さらに、CPU 10 は、押圧位置が登録ボタン 30 e であると判定した場合は、各入力欄 30 a 及び 30 b に入力されたユーザ名とパスワードをフラッシュメモリ 13 に記録し、記録が終了すると、ユーザ名とパスワードの登録処理を終了する。

【 0 0 2 9 】

次に、図 5 に示すフローチャートを参照して、情報処理装置 1 のメインルーチンについて説明する。

まず、電源ボタンが操作されて情報処理装置 1 の電源が投入されると、CPU 10 は、初期化処理を行う (ステップ S1)。この初期化処理において、CPU

10は、RAM11の予め定めた領域に認証フラグF=[0]を設定する。この初期化処理が終了すると、CPU10は、液晶駆動部14により操作画面40を表示画面3に表示させる(ステップS2)。ここで、図6は、操作画面40の一例を示す図である。

【0030】

このとき、CPU10は、認証処理を開始し(ステップS3)、その後、操作者によりペン型操作子2で表示画面3が押圧操作され、タッチパネル3bから押圧位置が通知されると(ステップS4: YES)、RAM11に格納した認証フラグFを参照する(ステップS5)。ここで、CPU10は、認証フラグFが[0]の場合は、ステップS3に処理を戻すのに対し、認証フラグFが[1]の場合は、タッチパネル3bから通知される押圧位置に基づいて対応する処理を行う(ステップS6)。

【0031】

具体的には、認証フラグFが[1]の場合、CPU10は、押圧位置が操作画面40(図4参照)の作業エリア40a内であると判定すると、液晶駆動部14により押圧位置に対応する位置の液晶表示パネル3aのドットを反転表示させ、押圧位置の軌跡を表示画面3に表示させる。また、CPU10は、押圧位置が操作画面40内のいずれかの操作ボタン40bであると判定した場合は、その操作ボタン40bに対応する処理を行う。例えば、押圧位置が「スケジューラ」ボタン40bの場合は、CPU10は、「スケジューラ」ボタン40bを反転表示させると共に、作業エリア40aにスケジュール画面を表示させる。

そして、CPU10は、タッチパネル3bから通知される押圧位置に基づいて対応する処理を行うと、ステップS3の処理に戻る。このように、CPU10は、ステップS3～S6までの処理を電源がオフされるまで繰り返し、操作者によりペン型操作子2で表示画面3が押圧操作される毎に認証フラグFを参照し、認証フラグFに応じて対応する処理を行うか否かを選択するようになっている。

【0032】

次に、図7及び図8に示すフローチャートを参照して、認証処理について説明する。

まず、CPU10は、情報処理装置1の電源投入後、液晶駆動部14によりログイン画面50を表示画面3に表示させる（ステップS10）。図9は、ログイン画面50の一例を示す図である。次に、CPU10は、タッチパネル3bから押圧位置が通知されると（ステップS11：YES）、押圧位置がログインボタン50eであるか否かを判定する（ステップS12）。ここで、ログイン画面50は、「ログイン」ボタン50eを有する点を除いて登録画面30（図4参照）とほぼ同一であるため、同一の部分は同一の符号を付して示している。すなわち、CPU10は、押圧位置が「ログイン」ボタン50e以外の位置の場合は、登録画面30の場合と同様の処理を行う（ステップS13）。操作者は、上述した登録画面30の場合と同様にして入力欄30a及び入力欄30bにユーザ名とパスワードを入力する。

【0033】

一方、CPU10は、押圧位置がログインボタン50eであると判定した場合は（ステップS12：YES）、入力されたユーザ名とパスワードがフラッシュメモリ13に記録されたユーザ名とパスワードと一致するか否かを判定する（ステップS14）。この判定において、一致しないと判定された場合は（ステップS14：NO）、CPU10は、ステップS11の処理に戻す。これに対して、入力されたユーザ名とパスワードがフラッシュメモリ13に記録されたものと一致すると判定した場合は（ステップS14：YES）、CPU10は、受信部15に受信開始を指示する（ステップS15）。

【0034】

次に、CPU10は、受信部15の受信結果に基づいて識別データID（以下、受信した識別データIDを「識別データIDa」という。）を受信したか否かを判定し（ステップS16）、識別データIDaを受信したと判定した場合は（ステップS16：YES）、受信した識別データIDaがROM14に記録された識別データIDと一致するか否かを判定する（ステップS17）。

【0035】

ここで、CPU10は、識別データIDaを受信しなかったと判定した場合（ステップS16：NO）若しくは受信した識別データIDaがROM14に記録さ

れた識別データIDと一致しなかった場合は（ステップS17：NO）、認証が得られないとして認証フラグFを[1]に設定する（ステップS18）。そして、CPU10は、認証フラグFを[1]に設定するとステップS16に処理を戻す。

一方、CPU10は、ステップS17において、受信した識別データIDaがROM14に記録された識別データIDと一致すると判定した場合は、認証が得られたとして認証フラグFを[0]に設定する（ステップS19）。そして、CPU10は、認証フラグFを[0]に設定すると、ステップS16に処理を戻す。

【0036】

以上のようにして、CPU10は、ステップS16→S17→S19→S16という処理か、ステップS16→（S17）→S18→S16という処理のいずれかを行う。これらの循環処理は、CPU10の処理速度からすれば、極めて速い循環処理になり、受信の有無の判断（ステップS16）および識別データの比較処理（ステップS17）は、実質的に継続して行われるのと同等となる。すなわち、上記の循環処理により、電源が投入された後はCPU10により、受信部15が受信した識別データIDaとROM12に記憶された内容との一致が継続的に判断される。

【0037】

このように、本願においては、使用に際して最初だけ判定するのではなく、実質的な意味で継続的に判定をしている。このため、この情報処理装置1は、正規のユーザが使用するペン型操作子2が情報処理装置1の近くに存在する間だけタッチパネル3bを介して入力したユーザの操作に対応する処理を行うことができる。従って、この情報処理装置1は、正規のユーザが装置から離れた場合などは、即座にその状況を検出することができ、不正使用者による入力を防止することができると共に、正規のユーザが装置の近くに帰ってくればすぐに使用を開始することができる。

【0038】

また、この情報処理装置1は、ペン型操作子2が近くにあれば使用できるので

、ペン型操作子2を持った正規のユーザが近くにいれば、他のペン型操作子を用いても使用することができる。従って、例えば、正規のユーザがその場で第三者に情報処理装置1を渡して第三者のペン型操作子を使って電話番号を入力してもらうといったことも従来機器と同様に行うことができる。すなわち、正規のユーザは、自分のペン型操作子2を身近に持っておけば、第三者の不正利用を確実に防止できるのである。

【 0 0 3 9 】

(2) 本願発明は、上述した実施形態に限らず種々の態様にて実施することができる。例えば、以下のような変形実施が可能である。

(2. 1)

上述の実施形態においては、CPU10の処理速度により識別データの受信判定と識別データの比較判定とが継続して行われるようにしたが、比較判定については、例えば、タイマ等を設け、このタイマの出力に同期して数秒おきに判定するようにしてもよい。

(2. 2)

上述の本実施形態においては、CPU10による認証の判定を所定間隔で行うようにしている。この場合、受信部15の受信動作を判定が行われるタイミングだけにすれば、消費電力の点で有利である。すなわち、受信部15に間欠駆動受信を行わせ、この間欠駆動のタイミングとCPU10による判定のタイミングを同期させるように構成してもよい。

(2. 3)

上述の実施形態においては、プログラムに基づくCPU10の処理によって識別データの比較判定を行った。これに対し、図10に示すように、識別データIDを記憶するレジスタ100と、受信した識別データIDaが転送されるレジスタ101を設け、これらのレジスタ100及び101の内容を比較するデジタルコンパレータ102によって、一致不一致を判定してもよい。すなわち、本発明の実施は、ソフトウェア処理によるばかりでなく、ハードウェアによっても実現することができる。

(2. 4)

上述の実施形態では、入力されたユーザ名とパスワード、及び受信した識別データIDに基づいて認証を行ったが、識別データIDのみに基づいて認証を行ってもよい。

【0040】

(2. 5)

上述の実施形態では、ペン型操作子2が継続して識別データを送信していたが、ペン型操作子2に受信部を設けると共に情報処理装置1に送信部を設けて、ペン型操作子2が、情報処理装置1から送信された識別データIDの送信要求を受信した場合のみ識別データIDを送信するようにしてもよい。この場合、ペン型操作子2の平均消費電力を小さくできるので、ペン型操作子2の駆動時間を長くすることができる。

【0041】

(2. 6)

上述の実施形態では、ペン型操作子2を用いて操作する情報処理装置に本発明を適用する場合について述べたが、要は、可搬操作子を用いて操作する情報処理装置であれば本発明を適用でき、タブレットやマウス等で操作する情報処理装置でもよい。なお、本発明は、セキュリティの観点から可搬操作子をユーザが携帯することが望ましいので、可搬操作子はコードレスの方がよい。また、本発明を適用できる情報処理装置には、パーソナルコンピュータ、PDA (Personal Digital Assistants) 等のプログラムを実行可能なコンピュータを含む。

【0042】

(2. 7)

上述の実施形態においては、認証処理を行うプログラムを予め情報処理装置1に記憶しておく場合について述べたが、図11に示すように、この認証プログラムを磁気記録媒体、光記録媒体、半導体記憶媒体などのコンピュータが読み取り可能な記録媒体に記録し、コンピュータが認証プログラムを読み取って実行するようにしてもよい。また、図12に示すように、この認証プログラムをサーバに格納し、ネットワークを介してサーバが送信要求のあったPCなどの端末に認証プログラムを送信するようにしてもよい。

【 0 0 4 3 】

【発明の効果】

上述したように本発明は、正規のユーザが使用する可搬操作子から送信される識別データに基づいて情報処理装置の近くに正規のユーザが存在するか否かを継続的に判定することにより、簡易かつ確実に第三者の不正利用を防止することができる。

【図面の簡単な説明】

【図 1】 本発明の実施形態に係る情報処理装置とペン型操作子の外観を示す図である。

【図 2】 情報処理装置の表示画面の構成を示す図である。

【図 3】 情報処理装置とペン型操作子の電氣的構成を示すブロック図である。

【図 4】 情報処理装置が表示する登録画面の一例を示す図である。

【図 5】 情報処理装置のメインルーチンのフローチャートである。

【図 6】 情報処理装置が表示する操作画面の一例を示す図である。

【図 7】 情報処理装置の認証処理の一部のフローチャートである。

【図 8】 情報処理装置の認証処理の一部のフローチャートである。

【図 9】 情報処理装置が表示するログイン画面の一例を示す図である。

【図 1 0】 変形実施例の説明に供する図である。

【図 1 1】 変形実施例の説明に供する図である。

【図 1 2】 変形実施例の説明に供する図である。

【符号の説明】

- 1 ……情報処理装置、
- 2 ……ペン型操作子、
- 2 a ……アンテナ、
- 3 ……表示画面、
- 3 a ……液晶表示パネル、
- 3 b ……タッチパネル
- 1 0 ……CPU、

1 1 …… RAM

1 2 …… ROM、

1 3 …… フラッシュメモリ、

1 4 …… 液晶駆動部、

1 5 …… 受信部、

1 6 …… 入出力部、

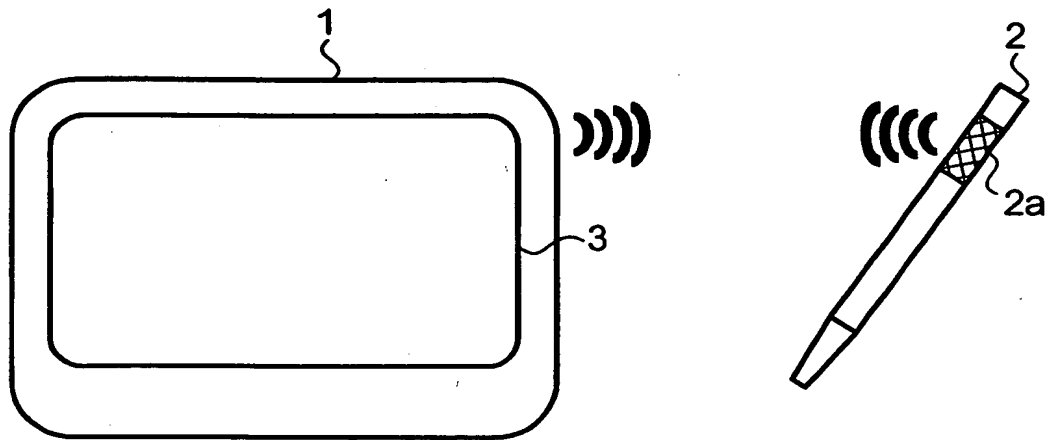
2 0 …… メモリ、

2 1 …… 送信部、

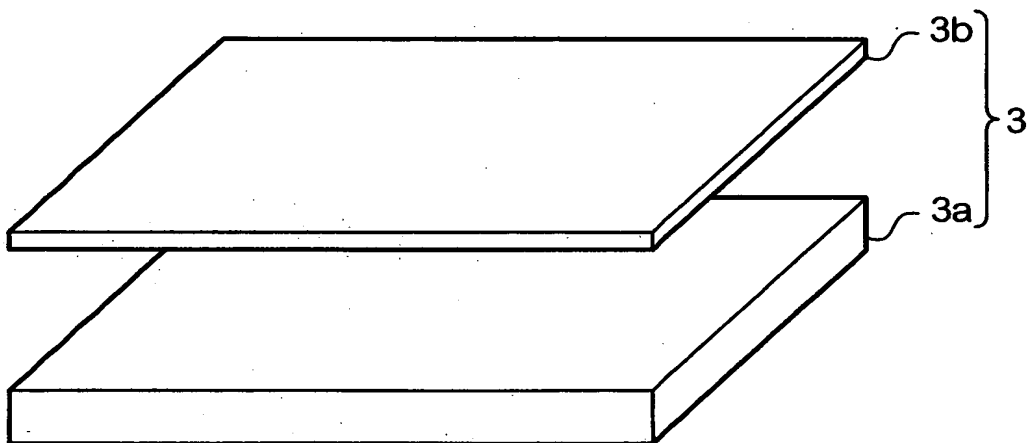
F …… 認証フラグ。

【書類名】 図面

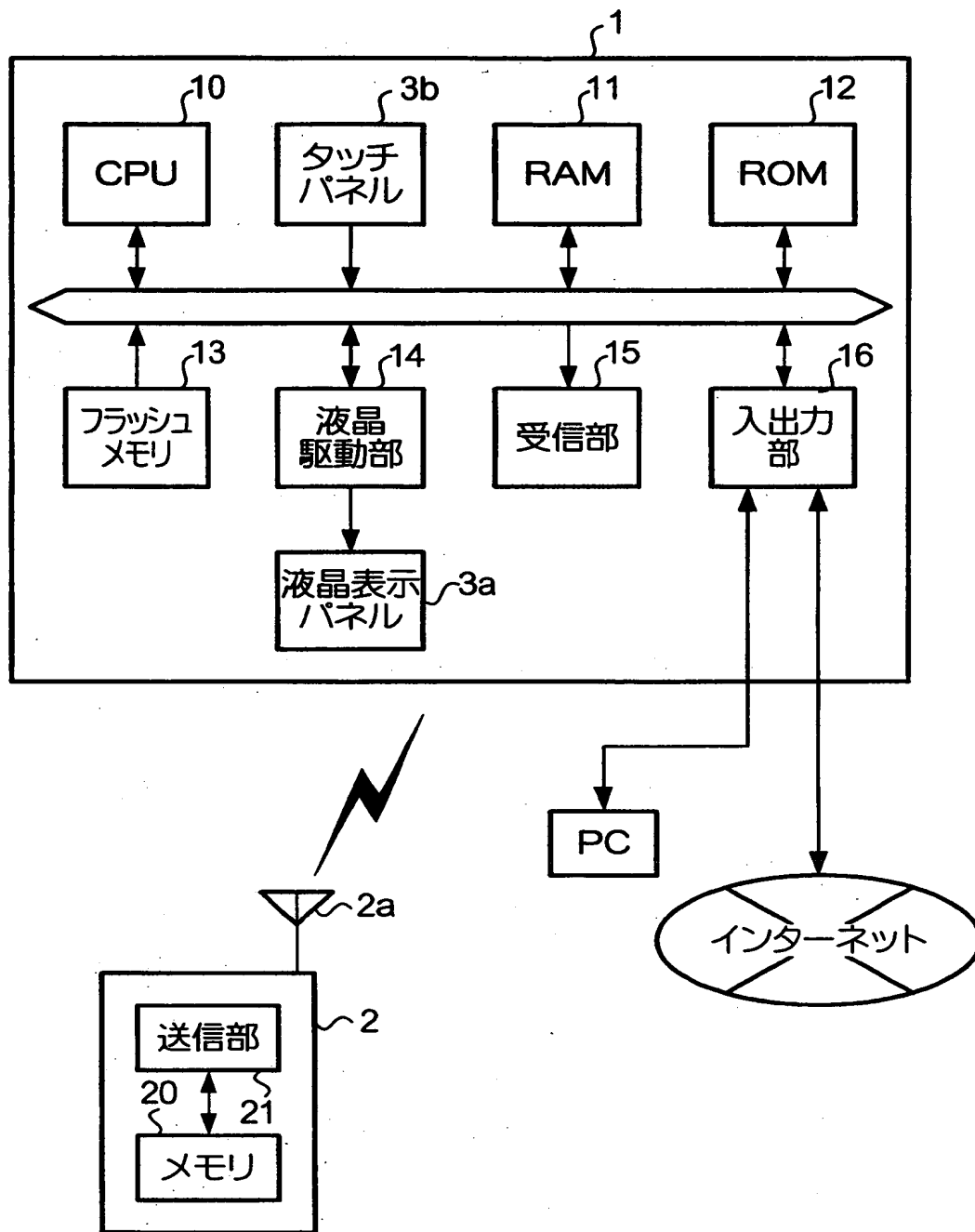
【図1】



【図2】



【図3】



【図 4】

30

ユーザ名 : 30a

パスワード: 30b

登録 30e
 キャンセル

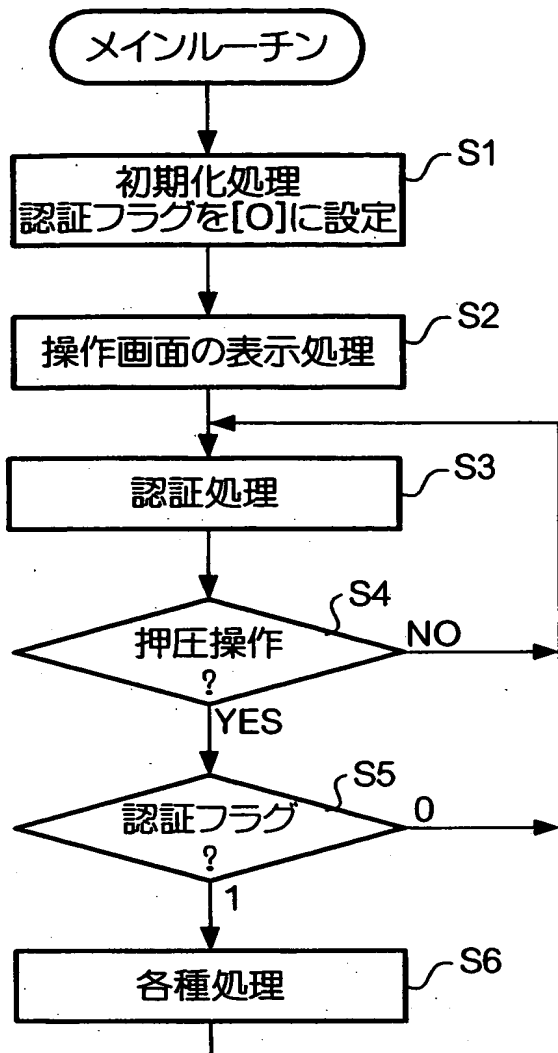
1	2	3	4	5	6	8	7	9	0
Q	W	E	R	T	Y	U	I	O	P
A	S	D	F	G	H	J	K	L	;
Z	X	C	V	B	N	M	,	.	/

30c

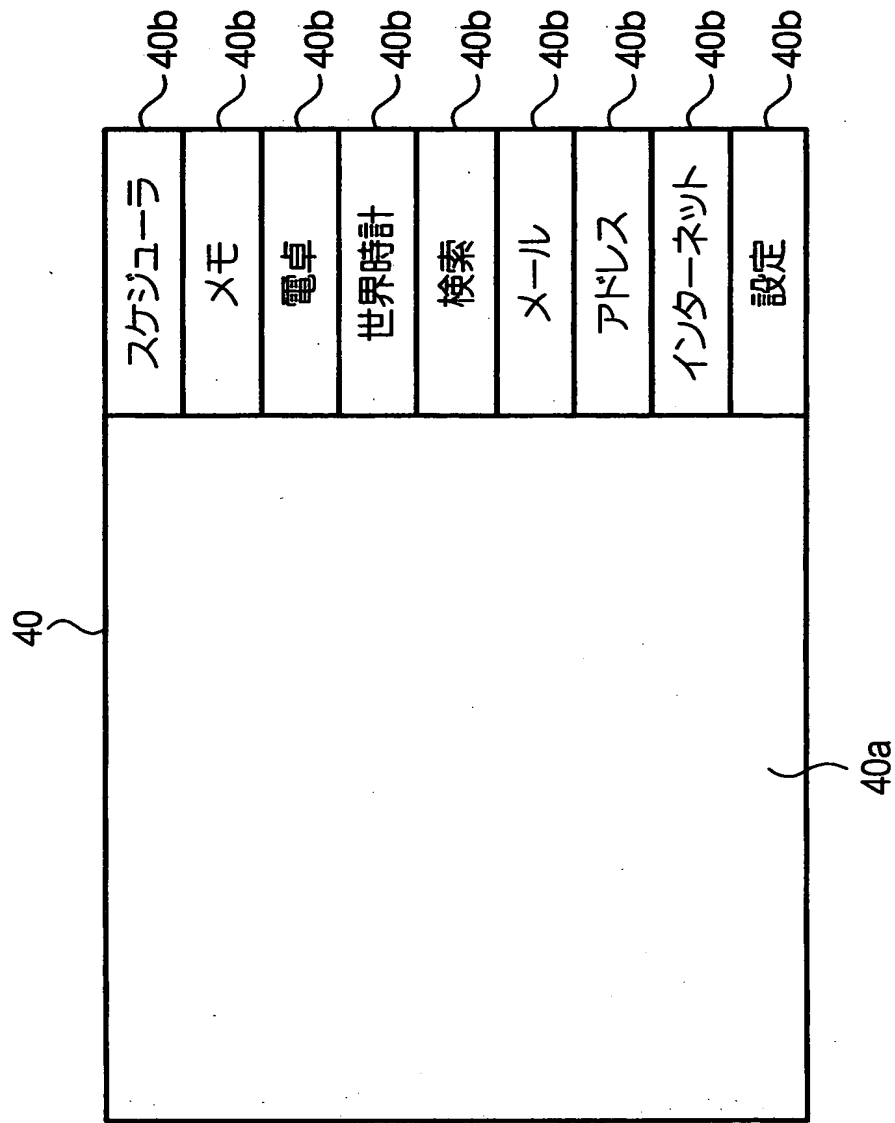
削除

 30d

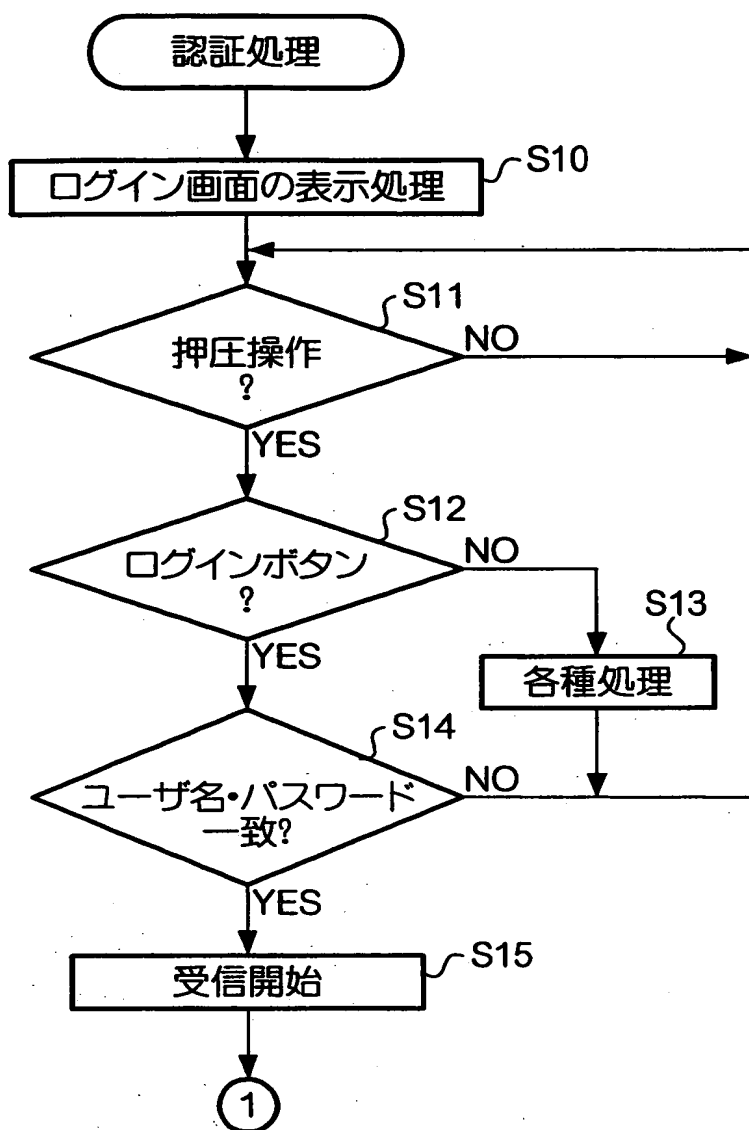
【図 5】



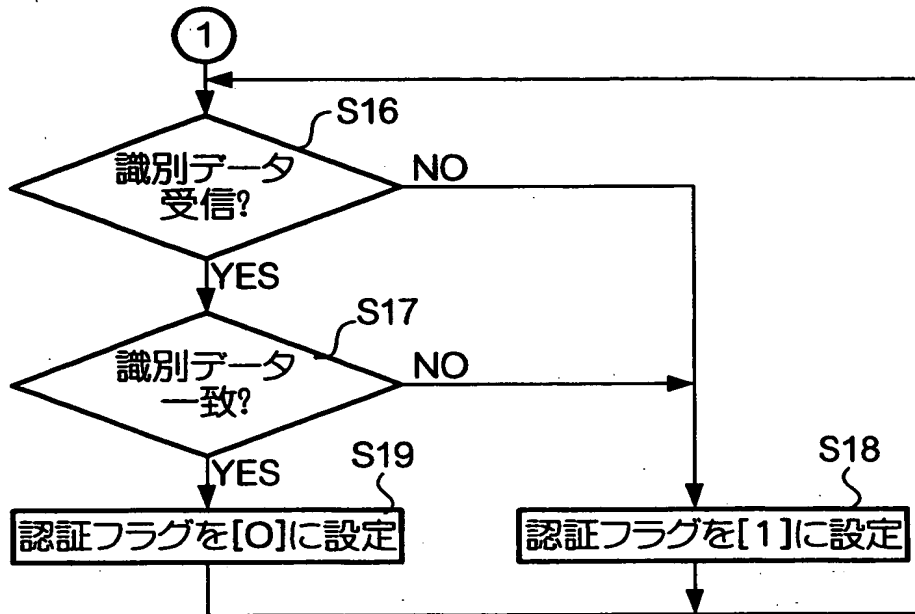
【図 6】



【図 7】



【図 8】



【図 9】

50

ユーザ名 : 30a

パスワード: 30b

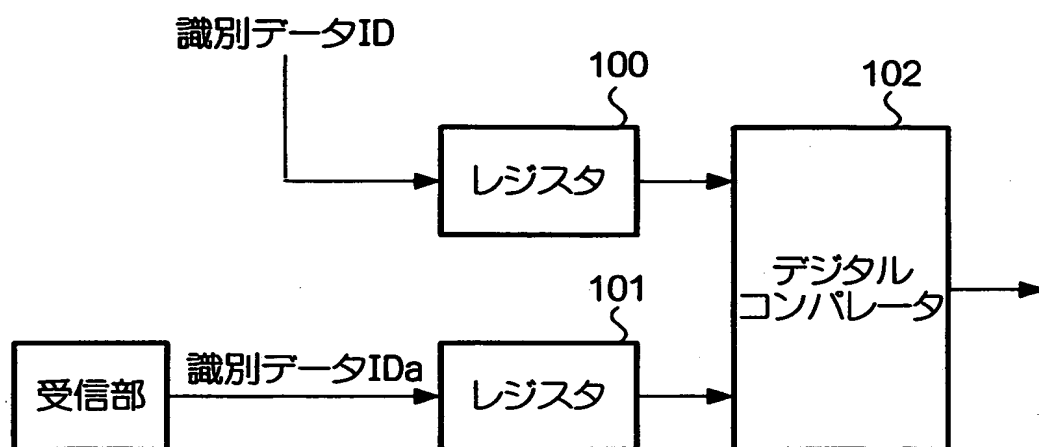
50e

1	2	3	4	5	6	8	7	9	0
Q	W	E	R	T	Y	U	I	O	P
A	S	D	F	G	H	J	K	L	;
Z	X	C	V	B	N	M	,	.	/

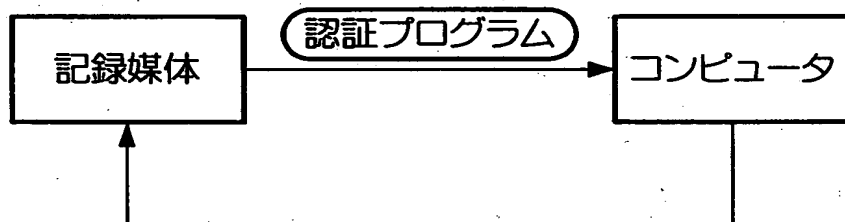
30c

30d

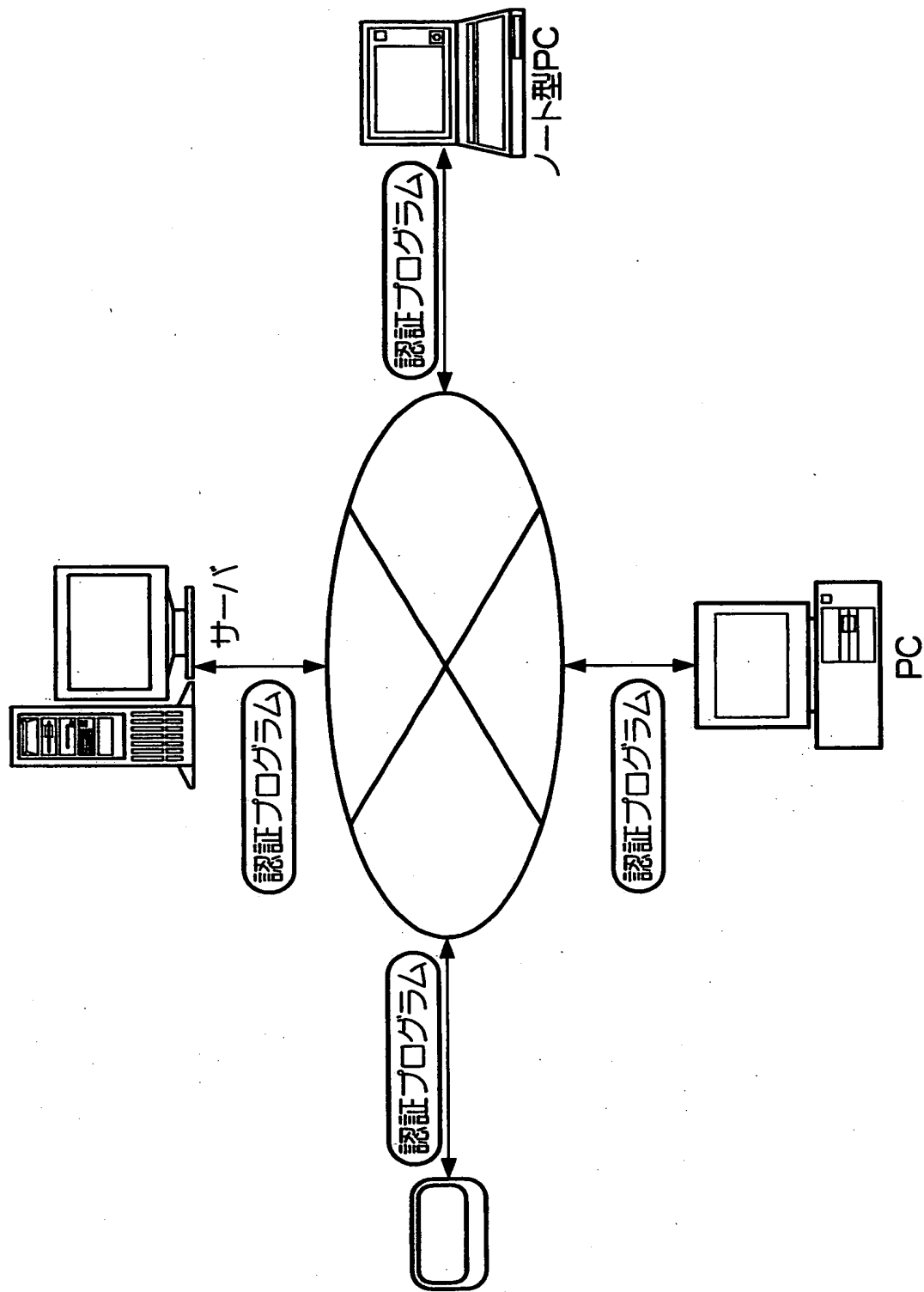
【図 1 0】



【図 1 1】



【図12】



【書類名】 要約書

【要約】

【課題】 簡易かつ確実に第三者の不正利用を防止することができる情報処理装置及び当該情報処理装置の制御方法、並びに制御プログラム及び当該制御プログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。

【解決手段】 情報処理装置 1 は、正規のユーザが使用する可搬操作子 2 から送信される識別データ I D に基づいて当該情報処理装置 1 の近くに正規のユーザが存在するか否かを継続的に判定し、該識別データ I D を受信していると判定する間だけユーザの操作に対応する処理を行う。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002369]

1. 変更年月日 1990年 8月20日
[変更理由] 新規登録
住 所 東京都新宿区西新宿2丁目4番1号
氏 名 セイコーエプソン株式会社